

Docket No. **8886.001.00**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: **Dennis Wayne HURST et al.**

FILING DATE: **Concurrently Herewith**

FOR: **INTERNET SECURITY ANALYSIS SYSTEM AND PROCESS**

**LIST OF INVENTORS' NAMES AND ADDRESSES**

ASSISTANT COMMISSIONER FOR PATENTS  
WASHINGTON, D.C. 20231

SIR:

Listed below are the names and addresses of the inventors for the above-identified patent application.

Dennis Wayne HURST  
515 Old Providence Ct.  
Alpharetta, GA 30004

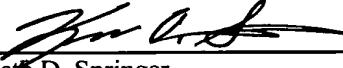
Darrin Ray BARRALL  
564 Cowan Rd.  
Conyers, GA 30094

Caleb Ikaki SIMA  
1103 Riverstone Place  
Woodstock, GA 30188

A declaration containing all the necessary information will be submitted at a later date.

Respectfully Submitted,

LONG ALDRIDGE & NORMAN LLP

  
\_\_\_\_\_  
Kenneth D. Springer  
Registration No. 39,843

Date: November 28, 2000

Sixth Floor  
701 Pennsylvania Avenue, N.W.  
Washington, D.C. 20004  
Tel. (202) 624-1200  
Fax. (202) 624-1298

S P E C I F I C A T I O N

TITLE OF THE INVENTION

INTERNET SECURITY ANALYSIS SYSTEM AND PROCESS

BACKGROUND OF THE INVENTION

5 1) Field of the Invention

This invention pertains to the field of computer security, and more particularly, to a system and process for analyzing potential security flaws in an Internet Web site.

2) Description of the Related Art

Increasingly, Internet Web sites are being exposed to external attack, or "hacking," which has been defined as the act of penetrating a closed computer system to gain access to knowledge and information that is contained within.

15 Individuals attack Web sites for a variety of reasons. A report by the United States Federal Bureau of Investigation (FBI) indicates that the originators of proprietary information theft can be classified into six categories. The report shows 35% of the criminals were discontented employees, 28% hackers, 18% other U.S. companies, 11% foreign companies, 20 8% foreign governments, and 10% miscellaneous. Examples of

some well-known attack methods include e-mail bombing, denial-of-service attacks, Trojan horses, worms, and simple back-door entry to a Web site. These attacks can not only cripple or shut down access to an attacked Web site, but can result in 5 unauthorized access to confidential customer information, including access passwords, and even credit card account numbers. The resulting damage to a commercial Web site can easily run into the millions of dollars.

According to the most recent FBI report, cyber crimes increased from 547 in 1998 to 1,154 in 1999. The FBI and the Computer Security Institute (Silicon Valley) found that 62% of information security officials reported security breaches in 1999 (National Journal's Technology Daily). These break-ins resulted in \$123 million losses from fraud, information theft, sabotage, and viruses.

Many companies use a proprietary base software product for conducting business and are focusing on tools for managing risk, and controlling sabotage against their applications. According to a Cyber-source study of online E-tailors, 75% 20 consider fraud to be a problem, and 62% consider it to be a serious problem. The NIPC, FBI, and United States Treasury, along with the President, have committed themselves to working along side the private sector in putting these concerns to

rest. Both the Economic Espionage Act of 1996, and the Theft of Trade Secrets Act (section 1832) have caused organizations to react promptly to damaging acts of violations.

Yet this problem is still not controlled and is in need 5 of counter-measures. In January of 2000, several denial-of-service (DOS) attacks occurred to well known E-commerce Web sites such as YAHOO® and E-BAY®. Incidents like this have brought the issue of Web site security directly into the public limelight. Of all the individuals polled on the questions of online banking, 65% stated that security was the main concern.

CONFIDENTIAL

Maintaining control of electronic fraud can be a time consuming process for E-commerce companies, banks, brokerage firms, and electronic billing/payment providers. Both the 15 network administrators and Web-masters do not have the proper tools to detect Web-based vulnerabilities. The complexity of information, separate system options, assessing the significance of penetrations, and a decision for correction is not prevalent in today's workplace. On-line fraud has a 20 special significance for an E-commerce site. The fear of security exploits can cause a negative impact on consumer confidence in an E-commerce site, which ultimately destroys the brand's image.

To prevent such attacks, Web site administrators manually search for and close potential security holes in their own Web sites. Because most Web sites undergo changes over time, and because new vulnerabilities and attack techniques are continually being developed, the Web site administrators must continually probe their sites for security weaknesses. This is time-consuming and fraught with the likelihood of undetected security flaws.

As the Internet continues to expand, more and more Web sites are being developed and operated by less experienced and trained personnel. And it becomes more and more difficult for all of these individuals to be knowledgeable in all of the latest techniques for hacking a Web site. This increases the potential for Web site security flaws to exist which can be exploited by hackers.

Accordingly, there is a need for an advanced Web security analysis system and process that can be used by Web site developers and administrators to identify security flaws in their Internet Web sites. It would also be advantageous to provide such a system and process which can be used by third party individuals who lack specific knowledge of an individual Web site's architecture and design. It would be further advantageous to provide such a system and process which is

automated, and which performs a security check without significant manual user intervention. Other and further objects and advantages will appear hereinafter.

SUMMARY OF THE INVENTION

5 The present invention comprises a system and process for analyzing potential security flaws in an Internet Web site.

In one aspect of the invention, an Internet security analysis system and process checks a target Internet Web site against a predetermined set of known exploits.

10 In another aspect of the invention, an Internet security analysis process is automated to execute without significant manual user interaction.

15 In yet another aspect of the invention, an Internet security analysis process is recursive, gathering information of security vulnerabilities and then exploiting that information to search for additional security vulnerabilities.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a functional block diagram

Figure 2 is a flowchart of a method of parsing through a Web site to identify possible security holes;

DESCRIPTION OF THE PREFERRED EMBODIMENTS

In a preferred embodiment, an Internet security analysis process is initiated by a Web site administrator for a target Web site to be analyzed. The process may be executed by an Internet security analysis system, which may be a personal computer having Internet access to the target Web site. Alternatively, a user may conduct the Internet security process through an Internet security analysis Web site. In that case, the Internet analysis system may be accessible via a Web server hosting the Internet security analysis Web site. Other embodiments are possible.

Figure 1 is a block diagram of a preferred embodiment of an Internet security analysis system 100 for performing a security analysis process for a target Web site. In a preferred embodiment, the Internet security analysis system 100 includes at least one central processing unit (CPU) 105 having associated therewith memory 110 and a mass data storage device 115, and optionally a display device 120, a data input device 125 (e.g., keyboard; mouse), and a network connection

device 130, all connected to each other via a communication bus 135. The data storage device 115 includes nonvolatile data storage means, such magnetic disk drive units, optical disk drive units, removable disk drive units, tape media, or 5 any combination thereof. The network connection device 130 includes hardware and software for establishing a data link connection between the Internet security analysis system 100 and a target Web site via the Internet. Preferably, the network connection device 130 includes circuitry to tie directly to the Internet via T1, T4 or similar high bandwidth data lines as would be understood by one skilled in the art.

20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
3310  
3311  
3312  
3313  
3314  
3315  
3316  
3317  
3318  
3319  
3320  
3321  
3322  
3323  
3324  
3325  
3326  
3327  
3328  
3329  
3330  
3331  
3332  
3333  
3334  
3335  
3336  
3337  
3338  
3339  
3340  
3341  
3342  
3343  
3344  
3345  
3346  
3347  
3348  
3349  
3350  
3351  
3352  
3353  
3354  
3355  
3356  
3357  
3358  
3359  
33510  
33511  
33512  
33513  
33514  
33515  
33516  
33517  
33518  
33519  
33520  
33521  
33522  
33523  
33524  
33525  
33526  
33527  
33528  
33529  
33530  
33531  
33532  
33533  
33534  
33535  
33536  
33537  
33538  
33539  
33540  
33541  
33542  
33543  
33544  
33545  
33546  
33547  
33548  
33549  
33550  
33551  
33552  
33553  
33554  
33555  
33556  
33557  
33558  
33559  
33560  
33561  
33562  
33563  
33564  
33565  
33566  
33567  
33568  
33569  
33570  
33571  
33572  
33573  
33574  
33575  
33576  
33577  
33578  
33579  
33580  
33581  
33582  
33583  
33584  
33585  
33586  
33587  
33588  
33589  
33590  
33591  
33592  
33593  
33594  
33595  
33596  
33597  
33598  
33599  
335100  
335101  
335102  
335103  
335104  
335105  
335106  
335107  
335108  
335109  
335110  
335111  
335112  
335113  
335114  
335115  
335116  
335117  
335118  
335119  
335120  
335121  
335122  
335123  
335124  
335125  
335126  
335127  
335128  
335129  
335130  
335131  
335132  
335133  
335134  
335135  
335136  
335137  
335138  
335139  
335140  
335141  
335142  
335143  
335144  
335145  
335146  
335147  
335148  
335149  
335150  
335151  
335152  
335153  
335154  
335155  
335156  
335157  
335158  
335159  
335160  
335161  
335162  
335163  
335164  
335165  
335166  
335167  
335168  
335169  
335170  
335171  
335172  
335173  
335174  
335175  
335176  
335177  
335178  
335179  
335180  
335181  
335182  
335183  
335184  
335185  
335186  
335187  
335188  
335189  
335190  
335191  
335192  
335193  
335194  
335195  
335196  
335197  
335198  
335199  
335200  
335201  
335202  
335203  
335204  
335205  
335206  
335207  
335208  
335209  
335210  
335211  
335212  
335213  
335214  
335215  
335216  
335217  
335218  
335219  
335220  
335221  
335222  
335223  
335224  
335225  
335226  
335227  
335228  
335229  
335230  
335231  
335232  
335233  
335234  
335235  
335236  
335237  
335238  
335239  
335240  
335241  
335242  
335243  
335244  
335245  
335246  
335247  
335248  
335249  
335250  
335251  
335252  
335253  
335254  
335255  
335256  
335257  
335258  
335259  
335260  
335261  
335262  
335263  
335264  
335265  
335266  
335267  
335268  
335269  
335270  
335271  
335272  
335273  
335274  
335275  
335276  
335277  
335278  
335279  
335280  
335281  
335282  
335283  
335284  
335285  
335286  
335287  
335288  
335289  
335290  
335291  
335292  
335293  
335294  
335295  
335296  
335297  
335298  
335299  
335300  
335301  
335302  
335303  
335304  
335305  
335306  
335307  
335308  
335309  
335310  
335311  
335312  
335313  
335314  
335315  
335316  
335317  
335318  
335319  
335320  
335321  
335322  
335323  
335324  
335325  
335326  
335327  
335328  
335329  
335330  
335331  
335332  
335333  
335334  
335335  
335336  
335337  
335338  
335339  
335340  
335341  
335342  
335343  
335344  
335345  
335346  
335347  
335348  
335349  
335350  
335351  
335352  
335353  
335354  
335355  
335356  
335357  
335358  
335359  
335360  
335361  
335362  
335363  
335364  
335365  
335366  
335367  
335368  
335369  
335370  
335371  
335372  
335373  
335374  
335375  
335376  
335377  
335378  
335379  
335380  
335381  
335382  
335383  
335384  
335385  
335386  
335387  
335388  
335389  
335390  
335391  
335392  
335393  
335394  
335395  
335396  
335397  
335398  
335399  
335400  
335401  
335402  
335403  
335404  
335405  
335406  
335407  
335408  
335409  
335410  
335411  
335412  
335413  
335414  
335415  
335416  
335417  
335418  
335419  
335420  
335421  
335422  
335423  
335424  
335425  
335426  
335427  
335428  
335429  
335430  
335431  
335432  
335433  
335434  
335435  
335436  
335437  
335438  
335439  
335440  
335441  
335442  
335443  
335444  
335445  
335446  
335447  
335448  
335449  
335450  
335451  
335452  
335453  
335454  
335455  
335456  
335457  
335458  
335459  
335460  
335461  
335462  
335463  
335464  
335465  
335466  
335467  
335468  
335469  
335470  
335471  
335472  
335473  
335474  
335475  
335476  
335477  
335478  
335479  
335480  
335481  
335482  
335483  
335484  
335485  
335486  
335487  
335488  
335489  
335490  
335491  
335492  
335493  
335494  
335495  
335496  
335497  
335498  
335499  
335500  
335501  
335502  
335503  
335504  
335505  
335506  
335507  
335508  
335509  
335510  
335511  
335512  
335513  
335514  
335515  
335516  
335517  
335518  
335519  
335520  
335521  
335522  
335523  
335524  
335525  
335526  
335527  
335528  
335529  
335530  
335531  
335532  
335533  
335534  
335535  
335536  
335537  
335538  
335539  
335540  
335541  
335542  
335543  
335544  
335545  
335546  
335547  
335548  
335549  
335550  
335551  
335552  
335553  
335554  
335555  
335556  
335557  
335558  
335559  
335560  
335561  
335562  
335563  
335564  
335565  
335566  
335567  
335568  
335569  
335570  
335571  
335572  
335573  
335574  
335575  
335576  
335577  
335578  
335579  
335580  
335581  
335582  
335583  
335584  
335585  
335586  
335587  
335588  
335589  
335590  
335591  
335592  
335593  
335594  
335595  
335596  
335597  
335598  
335599  
3355100  
3355101  
3355102  
3355103  
3355104  
3355105  
3355106  
3355107  
3355108  
3355109  
3355110  
3355111  
3355112  
3355113  
3355114  
3355115  
3355116  
3355117  
3355118  
3355119  
3355120  
3355121  
3355122  
3355123  
3355124  
3355125  
3355126  
3355127  
3355128  
3355129  
3355130  
3355131  
3355132  
3355133  
3355134  
3355135  
3355136  
3355137  
3355138  
3355139  
3355140  
3355141  
3355142  
3355143  
3355144  
3355145  
3355146  
3355147  
3355148  
3355149  
3355150  
3355151  
3355152  
3355153  
3355154  
3355155  
3355156  
3355157  
3355158  
3355159  
3355160  
3355161  
3355162  
3355163  
3355164  
3355165  
3355166  
3355167  
3355168  
3355169  
3355170  
3355171  
3355172  
3355173  
3355174  
3355175  
3355176  
3355177  
3355178  
3355179  
3355180  
3355181  
3355182  
3355183  
3355184  
3355185  
3355186  
3355187  
3355188  
3355189  
3355190  
3355191  
3355192  
3355193  
3355194  
3355195  
3355196  
3355197  
3355198  
3355199  
3355200  
3355201  
3355202  
3355203  
3355204  
3355205  
3355206  
3355207  
3355208  
3355209  
3355210  
3355211  
3355212  
3355213  
3355214  
3355215  
3355216  
3355217  
3355218  
3355219  
3355220  
3355221  
3355222  
3355223  
3355224  
3355225  
3355226  
3355227  
3355228  
3355229  
3355230  
3355231  
3355232  
3355233  
3355234  
3355235  
3355236  
3355237  
3355238  
3355239  
3355240  
3355241  
3355242  
3355243  
3355244  
3355245  
3355246  
3355247  
3355248  
3355249  
3355250  
3355251  
3355252  
3355253  
3355254  
3355255  
3355256  
3355257  
3355258  
3355259  
3355260  
3355261  
3355262  
3355263  
3355264  
3355265  
3355266  
3355267  
3355268  
3355269  
3355270  
3355271  
3355272  
3355273  
3355274  
3355275  
3355276  
3355277  
3355278  
3355279  
3355280  
3355281  
3355282  
3355283  
3355284  
3355285  
3355286  
3355287  
3355288  
3355289  
3355290  
3355291  
3355292  
3355293  
3355294  
3355295  
3355296  
3355297  
3355298  
3355299  
3355300  
3355301  
3355302  
3355303  
3355304  
3355305  
3355306  
3355307  
3355308  
3355309  
3355310  
3355311  
3355312  
3355313  
3355314  
3355315  
3355316  
3355317  
3355318  
3355319  
3355320  
3355321  
3355322  
3355323  
3355324  
3355325  
3355326  
3355327  
3355328  
3355329  
3355330  
3355331  
3355332  
3355333  
3355334  
3355335  
3355336  
3355337  
3355338  
3355339  
3355340  
3355341  
3355342  
3355343  
3355344  
3355345  
3355346  
3355347  
3355348  
3355349  
3355350  
3355351  
3355352  
3355353  
3355354  
3355355  
3355356  
3355357  
3355358  
3355359  
3355360  
3355361  
3355362  
3355363  
3355364  
3355365  
3355366  
3355367  
3355368  
3355369  
3355370  
3355371  
3355372  
3355373  
3355374  
3355375  
3355376  
3355377  
3355378  
3355379  
3355380  
3355381  
3355382  
3355383  
3355384  
3355385  
3355386  
3355387  
3355388  
3355389  
3355390  
3355391  
3355392  
3355393  
3355394  
3355395  
3355396  
3355397  
3355398  
3355399  
3355400  
3355401  
3355402  
3355403  
3355404  
3355405  
3355406  
3355407  
3355408  
3355409  
3355410  
3355411  
3355412  
3355413  
3355414  
3355415  
3355416  
3355417  
3355418  
3355419  
3355420  
3355421  
3355422  
3355423  
3355424  
3355425  
3355426  
3355427  
3355428  
3355429  
3355430  
3355431  
3355432  
3355433  
3355434  
3355435  
3355436  
3355437  
3355438  
3355439  
3355440  
3355441  
3355442  
3355443  
3355444  
3355445  
3355446  
3355447  
3355448  
3355449  
3355450  
3355451  
3355452  
3355453  
3355454  
3355455  
3355456  
3355457  
3355458  
3355459  
3355460  
3355461  
3355462  
3355463  
3355464  
3355465  
3355466  
3355467  
3355468  
3355469  
3355470  
3355471  
3355472  
3355473  
3355474  
3355475  
3355476  
3355477  
3355478  
3355479  
3355480  
3355481  
3355482  
3355483  
3355484  
3355485  
3355486  
3355487  
3355488  
3355489  
3355490  
3355491  
3355492  
3355493  
3355494  
3355495  
3355496  
3355497  
3355498  
3355499  
3355500  
3355501  
3355502  
3355503  
3355504  
3355505  
3355506  
3355507  
3355508  
3355509  
3355510  
3355511  
3355512  
3355513  
3355514  
3355515  
3355516  
3355517  
3355518  
3355519  
3355520  
3355521  
3355522  
3355523  
3355524  
3355525  
3355526  
3355527  
3355528  
3355529  
3355530  
3355531  
3355532  
3355533  
3355534  
3355535  
3355536  
3355537  
3355538  
3355539  
3355540  
3355541  
3355542  
3355543  
3355544  
3355545  
3355546  
3355547  
3355548  
3355549  
33555410  
33555411  
33555412  
33555413  
33555414  
33555415  
33555416  
33555417  
33555418  
33555419  
33555420  
33555421  
33555422  
33555423  
33555424  
33555425  
33555426  
33555427  
33555428  
33555429  
33555430  
33555431  
33555432  
33555433  
33555434  
33555435  
33555436  
33555437  
33555438  
33555439  
33555440  
33555441  
33555442  
33555443  
33555444  
33555445  
33555446  
33555447  
33555448  
33555449  
33555450  
33555451  
33555452  
33555453  
33555454  
33555455  
33555456  
33555457  
33555458  
33555459  
33555460  
33555461  
33555462  
33555463  
33555464  
33555465  
33555466  
33555467  
33555468  
33555469  
33555470  
33555471  
33555472  
33555473<br

identify security flaws. Preferably, the security analysis process executes a method of parsing through a target Web site to search for common security flaws. For example, in a preferred embodiment, the method includes analyzing the hyper-  
5 text markup language (HTML) script for the Web pages of the Web site and searching for commented-out references. Such commented-out references may include uniform resource locators (URLS) of Internet addresses for Web pages or other objects which are not intended to be accessed by a visitor to the Web site. Such Web pages or objects may contain data resident on a server hosting the target Web site which is not intended to be available to a visitor. As another example, in a preferred embodiment, the method includes bombarding the data entry fields of any Web forms of the target Web site with data in an attempt to break the target Web site.

10  
20  
25  
30  
35  
40  
45  
50  
55  
60  
65  
70  
75  
80  
85  
90  
95

20 A flowchart for a preferred embodiment process 200 of automatically parsing through a target Web site to identify possible security holes is shown in Figure 2. The process 200 may be initiated by a user and executed by a software program running on the Internet security analysis system 100, which as described above may be preferably a standalone user computer, or a computer accessible to a user via the Internet, etc. Typically, the process 200 is initiated by an administrator of the target Web site.

In a first step 205, an Internet security analysis computer establishes an Internet connection with a Web server hosting an Internet Web site for which a security inspection will be performed (the "target Web site"). The Internet security analysis computer retrieves a default Web page for the target Web site, e.g., "Index.html."

In a step 210, the Internet security analysis system 100 parses through the script (e.g., HTML code) for the default Web page to search for any linked-to Web pages or other objects which are referenced. The URL or address of each linked-to Web page is then stored in a database at the Internet security analysis computer. In particular, the Internet security analysis computer parses through Web pages looking for anchor links and JAVASCRIPT® links.

15 In a step 215, each linked-to Web page is then in turn retrieved by the Internet security analysis computer and the script for the retrieved Web page is parsed to search for any further linked-to Web pages. This process is repeated for each link and each linked-to Web page that is found.

20 Preferably, the "depth" of linked-to Web pages which are retrieved may be set by a user to any value, so that only first or second level linked-to Web pages may be retrieved. Alternatively, only linked-to Web pages which are hosted on a

same server, or which have a same domain address, as the default Web page may be retrieved.

As a result of the steps 205-215, the Internet security analysis system builds a valid Web page database with an 5 entire map of the valid Web pages of the target Web site.

Then, in a step 220, the default Web page for the target Web site is parsed for any hidden Uniform Resource Locators (URLs), such as commented-out code, or any reference to a file or Web page that is not linked-to (or HREF'ed). These hidden URLs are then checked against the valid Web page database to insure that the Internet security analysis system has not already retrieved the corresponding hidden Web page or object. If the corresponding hidden Web page or object has not previously been retrieved, then the address is stored in a prioritized database of "vulnerable" Web pages at the Internet security analysis computer. 15

In a step 225, each hidden Web page or object is then in turn retrieved by the Internet security analysis system and the script is parsed to search for any further hidden URL's. 20 If any further hidden URL's are found, then the Internet security analysis system retrieves the corresponding hidden Web page or object for the hidden URL and parses through it to

search for any still further hidden URLs. This process is repeated for each link and each linked-to Web page or object that is found.

As a result of the steps 220-225, the Internet security analysis system builds a vulnerable Web page database with an entire map of the "vulnerable" Web pages of the target Web site. Together, the steps 205-225 constitute a "Webcrawl" of the entire target Web site, performed by parsing through each retrieved Web page in turn to find additional links.

Preferably, when the Internet security analysis system 100 parses through each retrieved Web page, it performs a keyword search to detect points of interest. For instance, if a Web page is retrieved thru the Webcrawl with the word "admin" located in the Web page, the Internet security analysis system 100 will flag it as a "point of interest" and name it as "possible administration Web page."

Then, in a step 230, the Internet security analysis system 100 checks a predetermined - but extensible - list of known, common security vulnerabilities. Typically, these 20 security vulnerabilities are "exploits" which have become well known to security experts. The Internet security analysis

system scans the target Web site to determine whether or not any of the exploits are present at the target Web site.

For example, assume a case where the following three security vulnerabilities are to be checked:

5        /security/exploit.asp  
          /security/vuln.asp  
          /security/b00m.asp

In that case, the Internet security analysis system will issue a request to the target Web site for the directory "security." The Web server for the target Web site will issue either a true or false response, depending on whether the directory exists or not. If the response is true (indicating that the directory does exist), then the above-mentioned three security vulnerabilities are checked to determine whether they exist.

15        In the above case, it is also possible to perform a keyword search on each response received to detect points of interest. For instance, if a response is received with the keyword "<DIR>" included, the Internet security analysis system 100 will flag it as a vulnerability.

As another example, assume that the "Webcrawl" in the steps 205-225 retrieved the URL "/scripts/db/msadcs.dll" and stored it in the vulnerable Web pages database, and that "/msadc/msadcs.dll" is stored in the list of known, common 5 security vulnerabilities. In that case, in the step 230, the Internet security analysis system 100 takes the actual filename of the check (msadcs.dll) and flags it as being present in "/scripts/db/msadcs.dll." This allows the Internet security analysis system 100 to find a security vulnerability even though it is out of its normal location. Once a security vulnerability is found in an alternate directory the Internet security analysis system 100 will check for other files that typically reside with the file that was found. For example, if "msadcs.dll" is usually in a folder that also contains "msadcs2.dll", then the Internet security analysis system 100 would also check for the existence of "msadcs2.dll" in the "/scripts/db" folder where "msadcs.dll" was found.

Another security vulnerability check which may be employed by the Internet security analysis system 100 is 20 common file name checking. For example, the Internet security analysis system 100 will recursively try to request WS\_FTP.LOG from all directories retrieved from the Webcrawl.

Yet another security vulnerability check which may be employed by the Internet security analysis system 100 is port scanning (scanning a machine for open ports) integrated with Web server discovery. By taking the information retrieved 5 from a port scanner (port open on any given host) the Internet security analysis system 100 will attempt to determine whether that port is supporting HTTP or HTTPS. If the port returns valid on any HTTP or HTTPS request then the server is marked as a Web server sitting on that specific port. The Internet security analysis system 100 will go through an entire range of hosts, trying each port with this method. When completed, the Internet security analysis system 100 will have a list of hosts that are currently hosting a Web server and the port or ports on which the Web server is listening. The Internet security analysis system 100 will then take this list and pass it to the "Webcrawl engine" portion of the Internet security analysis system 100. This allows an easy ability to scan an entire network and look for Web vulnerabilities

20 If a security vulnerability exists, then in a step 235 a record of the security vulnerability is added to a security vulnerability database maintained at the Internet security analysis system 100.

Accordingly, an efficient and intelligent vulnerability search is conducted. Because a Web site may be very large and contain hundreds or more Web pages and dozens or more exploits must be checked, the above-described process of determining 5 the appropriateness of a security check before actually issuing the check greatly expedites the automated security check process.

Advantageously, in a step 240 the Internet security analysis system further exploits each of the vulnerabilities detected in the step 235 and added to the security vulnerability database to search for further security vulnerabilities and to gather other information regarding the target Web site. This process is recursively repeated until no new data is obtained.

15 In a step 245, the Internet security analysis system applies a predetermined - but extensible - list of hack methods to the data which was retrieved in the steps 205-240 to identify security vulnerabilities.

20 In a preferred embodiment, a first hack method comprises the Internet security analysis system issuing a series of requests, such as:

GET/\$SERVER\_NAME/\$SCRIPT\_NAME?\$VAR1=/.../.../boot.ini

GET/\$SERVER\_NAME/\$SCRIPT\_NAME?\$VAR2=/.../.../boot.ini

5

These requests check every script name and variable at the target Web site for a "Directory traversal exploit." If any of these requests return a positive result, then a security vulnerability has been found.

In a second hack method, the Internet security analysis system searches for buffer overflows by issuing a series of requests such as:

GET/\$SERVER\_NAME/\$SCRIPT\_NAME?\$VAR1=AAAAAAA . . . (2048 more A'S)

15 GET/\$SERVER\_NAME/\$SCRIPT\_NAME?\$VAR2=AAAAAAA . . . (2048 more A'S)

20 These requests check every script name and variable at the target Web site for unexpected results in the case of a buffer

overflow. If any unexpected data is returned, then a security vulnerability has been found.

In a third hack method, the Internet security analysis system searches for old files or variables which are still present on a Web server for the target Web site, bit which are not intended to be available to a visitor. The Internet security analysis system searches issues a series of requests such as:

GET/\$SERVER\_NAME/\$SCRIPT\_NAME.old  
GET/\$SERVER\_NAME/\$SCRIPT\_NAME.bak  
GET/\$SERVER\_NAME/\$SCRIPT\_NAME.bac

These requests are issued for every script name and variable at the target Web site.

Although a preferred embodiment process includes the 15 three hack methods described above, additional hack methods are also possible and may be employed.

For example, where the Web site includes a Web form, intentionally invalid data may be entered into one or more data entry fields of the Web form and submitted to the Web 20 site to determine if any invalid or unexpected results are

produced by the Web site. This process may recursively submit various combinations of invalid data entered into the various data entry fields of the Web form. Once a security vulnerability is detected in this way, the data producing the 5 vulnerability may then be used as a starting point for testing all other Web forms at the target Web site.

Preferably, a user may also employ cookie or HTML manipulation to search for security vulnerabilities. The Internet security analysis system 100 will allow a user to intercept the communication between a browser and a Web server and give the user the option to change or manipulate the data being sent between the client and server before the data is actually sent. This allows a user to manipulate the communication in any way, including cookies and over SSL communication. The Internet security analysis system 100 allows a user to create an HTTP or HTTPS request from either an existing request that has already been send to the server or to create a new request on the fly, including the ability to add, modify or not send any of the following: the URL, 20 parameters that are sent to the server; any Header that is sent in the request; cookies that are sent to the server; and the method that is used to send the request (i.e.: HEAD, POST, GET).

If during the Webcrawl in the steps 205-225, the Internet security analysis system 100 encounters what it deems to be a login page, it will give the option to the user to "brute force" the login (try multiple logins and passwords until a successful one is retrieved), or to automate the login so that the Internet security analysis system 100 will brute force it automatically, and the user does not have to stop the scan and will brute force it automatically.

00000000000000000000000000000000  
Preferably, there are two methods of brute forcing a login screen it can either be a form login or a basic authorization "pop-up box" login.

The Internet security analysis system 100 also preferably supports passing of user defined user names and passwords that are sent to the target server. This facilitates testing of target Web sites that require a login name and password to gain access to the target Web site, or a folder on the target Web site.

Moreover, in some cases one or more of the above-20 described hack methods may not be used. Optionally, the user may choose the hack methods which are employed.

If any of security vulnerabilities have been found in the step 245, then in a step 250 the Internet security analysis system adds a record for the security vulnerability to the security vulnerability database.

5        Finally, in a step 255, the Internet security analysis system prioritizes all security vulnerabilities which have been identified in the steps 205-250, and presents the prioritized list to the user, for example on a computer display screen. For example, it is known that a "SQL server error" is high risk vulnerability, and accordingly, this will be communicated to the user via the prioritization. Preferably, the Internet security analysis system also suggests how the user may eliminate the detected security vulnerabilities.

15        In a preferred embodiment, a user may disable the automatic operation and instead control one or more aspects of how the Internet security analysis process executes. For example, the user may be allowed to change the values sent to the target Web site in the step 245. The user may also view 20 any malformed "cookies" which are returned during the Internet security analysis process. The user may manually edit and change the HTML code for any Web page which is retrieved from the Web site and then submit the changed Web page back to the

server for the target Web site. This facilitates scanning of applications where specific user interaction (e.g., username and password) are required to gain access to the application, or where an automated scan could be dangerous to the application. One example of an application where an automated scan could be dangerous would be administrative application that has elevated access to the target Web site.

While preferred embodiments are disclosed herein, many variations are possible which remain within the concept and scope of the invention. Such variations would become clear to one of ordinary skill in the art after inspection of the specification, drawings and claims herein. The invention therefore is not to be restricted except within the spirit and scope of the appended claims.